ISO 27001:2022 Information Security Policy Statement
Effective Date: January 2026

Introduction

EverSAFE Training Ltd is committed to protecting the confidentiality, integrity, and availability of all physical and digital information assets. This Information Security Policy is aligned with the ISO/IEC 27001:2022 standard and forms the foundation of our Information Security Management System (ISMS). It supports business continuity, regulatory compliance, and the protection of personal, corporate, and client data.

Purpose

The purpose of this policy is to:

- Establish a structured and risk-based approach to information security
- Protect sensitive information from unauthorised access, modification, or loss
- Ensure business continuity and the integrity of services
- Comply with all applicable data protection, cyber security, and contractual obligations

Scope

This policy applies to:

- All employees, contractors, and temporary staff
- All business functions and third-party suppliers with access to information systems
- All information assets, systems, networks, devices, and data managed or processed by EverSAFE

Key Information Security Objectives

- Achieve 100% compliance with mandatory information security training
- Maintain business continuity through tested incident response and recovery plans
- Achieve zero unauthorised access incidents annually
- Ensure secure onboarding/offboarding of staff and partners

Governance and Roles

Information Security Officer (ISO): Oversees the implementation and monitoring of the ISMS.Senior Leadership: Provides strategic direction and ensures adequate resourcing.All Staff: Must follow information security procedures, attend training, and report incidents promptly.

Information Security Controls

EverSAFE employs a layered approach to information security:

- Access Control: Role-based user access, password policies, two-factor authentication
- Asset Management: Inventory and classification of all devices, documents, and systems
- Encryption: Data at rest and in transit encrypted to UK industry standards
- Physical Security: Secure premises, CCTV, controlled visitor access
- Patch Management: Timely updates and vulnerability scanning

Risk Management

We maintain an Information Asset Register and conduct regular risk assessments. Controls are applied proportionate to risk levels. Mitigation measures include:

- Antivirus and firewall protection
- Cloud-based data backups with redundancy
- Restricted administrative access

Incident Response

All incidents are reported to the Information Security Officer. The Incident Response Plan includes:

- Initial triage and containment
- Root cause analysis
- Communication with affected parties
- Review and improvement actions
- Report all suspected breaches immediately via: hello@eversafetraining.co.uk

Legal and Regulatory Compliance

We comply with:

- UK GDPR and Data Protection Act 2018
- Computer Misuse Act 1990
- Cyber Essentials requirements
- Client-specific contractual security obligations

Supplier Security

Third-party vendors with access to sensitive information are:

- Vetted during procurement
- Bound by contractual security clauses
- Reviewed annually for continued compliance

Training and Awareness

All staff complete mandatory security awareness training on induction and annually. Topics include:

- Phishing and social engineering
- Safe handling of data
- Secure device use and remote access protocols

Monitoring and Review

The ISMS is subject to:

- Annual internal audits
- Periodic penetration testing
- Executive-level management reviews
- Continual improvement processes

Policy Review

This policy will be reviewed at least annually or upon significant operational, technological, or legal changes.

- Approved by: Managing Director
- Approval Date: January 2026
- Next Review Due: January 2027
- Version: 2.0
- Document Owner: Hayley Everingham